Über die quadratischen Zahlkörper mit Primzerlegung

Von LADISLAUS RÉDEI in Szeged

Die Zahlen $-4, \pm 8$ und $\pm p$ ($\equiv 1 \pmod 4$, p rationale Primzahl) nennen wir *Stammdiskriminanten*. Offenbar zerlegt sich die Diskriminante D eines (absolut) quadratischen Zahlkörpers eindeutig in ein Produkt von Stammdiskriminanten, die wir deshalb die *Stammdiskriminantenfaktoren* von D nennen dürfen. Es gilt der

Satz. *Die Diskriminante D eines quadratischen Zahlkörpers Q mit Primzerlegung ist entweder eine Stammdiskriminante oder das Produkt von zwei negativen Stammdiskriminanten.*

In etwas weniger scharfen Form war dieser Satz bekannt und spielt in der Erforschung des Euklidischen Algorithmus in quadratischen Zahlkörpern eine Rolle. Vier Beweise liegen für ihn schon vor, und zwar ein klassenkörpertheoretischer (BEHRBOHM und RÉDEI [1]), ein idealtheoretischer (INKERI [2]), ferner ein elementarer, aber etwas mühsamer, und ein sehr kurzer, auf dem Satz von DIRICHLET fußender (ENNOLA [3]). Der dritte dieser Beweise hat uns zu einem weiteren, ebenfalls elementaren und sehr leichten Beweis angeleitet, der zugleich obige Verschärfung hergab.

Mit R werde der Ring der ganzen Elemente von Q bezeichnet. Die Voraussetzung hat zur Folge, daß irgend zwei Elemente α, β von R einen (bis auf Assoziierte bestimmten) größten gemeinsamen Teiler in R haben, den wir mit (α, β) bezeichnen.

$\alpha \sim \beta$ bezeichnet, daß α, β assoziierte Elemente von R sind.

E und E^2 bezeichnen die Gruppe der Einheiten bzw. der Einheitenquadraten von R. Im Fall $D > 0$ bezeichnet ε die Grundeinheit (> 1) von R.

N bezeichnet die Norm der Elemente von Q.

Für ein Element α von Q bezeichnet α' das Konjugierte von α. Also besteht $N(\alpha) = \alpha\alpha'$.

Lateinische Minuskeln bezeichnen ganze rationale Zahlen. Insbesondere bezeichnen p, q verschiedene (positive) Primzahlen, ferner bezeichnet m den

quadratfreien Kern von D. Dies bedeutet $D=m$ für $2\nmid D$ und $D=4m$ für $2|D$. Stets ist also sowohl $\sqrt{D}$ als auch $\sqrt{m}$ ein erzeugendes Element von Q.

Beim Beweis dürfen wir uns auf die D beschränken, die keine Stammdiskriminanten sind. Zu beweisen ist dann, daß D das Produkt von zwei negativen Stammdiskriminanten ist.

Hilfssatz. *Wenn $p|D$ ist, so gibt es ein $\eta(\in E)$ mit $\sqrt{p\eta}\in Q$.*

Um dies zu beweisen unterscheiden wir die zwei Fälle

$$p|m \quad \text{bzw.} \quad p\nmid m \,(\text{also } p=2,\ m\equiv -1 \pmod 4).$$

Entsprechend setzen wir

$$\alpha=(p,\sqrt{m}) \quad \text{bzw.} \quad \alpha=(2,1+\sqrt{m}).$$

Dann ist

$$\alpha^2=(p^2,m) \quad \text{bzw.} \quad \alpha^2=(4,1+m+2\sqrt{m})=(4,2\sqrt{m}),$$

also in beiden Fällen $\alpha^2\sim p$, d. h. $\alpha^2=p\eta$ mit einem $\eta(\in E)$. Wegen $\alpha\in Q$ gilt dabei auch $\sqrt{p\eta}\in Q$. Somit ist der Hilfssatz bewiesen.

Wenn nun $D<0$ ist, so muß, da D keine Stammdiskriminante ist, sogar $D<-4$ gelten. Folglich besteht E aus 1 und -1. Da aber Q imaginär ist, kommt im Hilfssatz nur $\eta=-1$ in Frage. Hiernach sollte Q alle $\sqrt{-p}$ $(p|D)$ enthalten. Da dies falsch ist, ist der Fall $D<0$ gar nicht möglich.

Es ist nur noch der Fall $D>0$ übrig. Im Hilfssatz muß jetzt $\eta>0$ gelten. Da ferner η nur mod ε^2 in Frage kommt, so darf $\eta=1$ oder $\eta=\varepsilon$ angenommen werden.

Wenn dabei für ein p der Fall $\eta=1$ zutrifft, so folgt $\sqrt{p}\in Q$, $m=p$, $D=4p$, $p\neq 2$. Hiernach gilt jetzt die Stammdiskriminantenzerlegung $D=-4\cdot -p$. Somit ist der Satz für diesen Fall bewiesen.

Zu betrachten ist nur noch der Fall, daß im Hilfssatz stets $\eta=\varepsilon$ gilt, d. h. alle $\sqrt{p\varepsilon}\,(p|D)$ in Q liegen. Dies zunächst nur für ein p berücksichtigend, ergibt sich hierfür $\sqrt{p\varepsilon'}\in Q$, $\varepsilon'>0$, also

$$N(\varepsilon)=1.$$

Gelten ferner $p|D$ und $q|D$, so folgt $\sqrt{p\varepsilon}\ \sqrt{q\varepsilon}\in Q$, $\sqrt{pq}\in Q$,

$$m=pq.$$

Da hierdurch p und q (bis auf die Reihenfolge) eindeutig bestimmt sind, so kann D außer p und q überhaupt keine weiteren Primteiler haben. Das bedeutet, daß D nur zwei Stammdiskriminantenfaktoren hat. Diese sind (wegen $D>0$) von gleichem Vorzeichen. Wir nehmen an, daß sie positiv sind; durch einen hieraus abzuleitenden Widerspruch wird der Satz bewiesen sein.

Wegen der Annahme ist jedes von p und q entweder kongruent 1 mod 4 oder gleich 2. Also besteht eine Gleichung

$$pq = a^2 + b^2 \qquad (2 \nmid a).$$

Man setze

$$\varrho = b + \sqrt{pq}, \quad \omega = (a, \varrho).$$

Dann gelten

$$\varrho\varrho' = -a^2, \quad (\varrho, 2) \sim 1, \quad (\varrho, \varrho') \sim 1,$$

also

$$\omega^2 = (a^2, \varrho^2) = (\varrho\varrho', \varrho^2) \sim \varrho.$$

Hiernach ist $\omega^2\varrho^{-1}$ ein Element von E mit negativer Norm. Dies ist aber wegen $N(\varepsilon) = 1$ unmöglich. Durch diesen Widerspruch ist der Satz bewiesen.

Literaturverzeichnis

[1] H. Behrbohm und L. Rédei, Der Euklidische Algorithmus in quadratischen Zahlkörpern *J. reine angew. Math.*, **174** (1936), 192—205.

[2] K. Inkeri, Neue Beweise für einige Sätze zum Euklidischen Algorithmus in quadratischen Zahlkörpern, *Ann. Univ. Turkensis*, A IX, **1** (1948).

[3] V. Ennola, Two elementary proofs concerning simple quadratic fields, *Nordisk mat Tidskrift*, **6** (1958), 114 - 117.

(Eingegangen am 27. September 1959)